Argentina's Protection of Personal Data: Initiation and Response

MAXIM GAKH*

ABSTRACT

In response to a changing global privacy law regime, and specifically the passage of the European Union Directive setting standards for the protection of personal data, Argentina has been at the forefront of Latin American legal efforts to increase privacy. Argentina's efforts began with the enactment of a constitutional provision that created the habeas data cause of action, allowing for injunctive relief for those seeking access, modification, or suppression of personal data. After an unsuccessful attempt, the Law for the Protection of Personal Data was finally ratified in 1998 and went into effect in 2000. The Law for the Protection of Personal Data provides the statutory framework for the habeas data cause of action and establishes specific rights of data owners and obligations of data users. The Law for the Protection of Personal Data also establishes a controlling administrative agency charged with its implementation and assuring the protection of personal data. The European Union has since determined that Argentina's personal data protection regime is "adequate" for international data transfers in accordance with its Directive. As a result of this unique approach of protecting personal data, Argentina is now setting a trend for other countries in Latin America and worldwide.

I. INTRODUCTION

In order to protect personal data and prevent data transfers to countries with inadequate personal data protection, the European Union ("EU") has created policies for its member states to implement. The United States, on the other hand, has chosen a deregulatory approach to protecting personal data. A safe harbor permitting the transfer of personal data from the United States to the EU under certain conditions has thus far bridged these divergent approaches. But a new method of protecting personal data is gaining force. It involves combining a cause of action allowing individuals to sue in order to access, suppress, or correct already collected information with

* Maxim Gakh is a candidate for a juris doctor at The Ohio State University Moritz College of Law, class of 2007. The author has an A.B. with a major in political science from Washington University in St. Louis.

a set of standards—which adhere to the EU Directive—to assure that personal data is being responsibly maintained. The stage for this new development is Latin America, and Argentina is in the lead. Since Argentina was originally scheduled to host the 28th International Conference of Data Protection and Privacy Commissioners in Buenos Aries in 2006,[1] and Argentina is the first country in Latin America, and one of only a handful worldwide, deemed to provide "adequate" personal data protection by the EU, its data protection regime is critical for understanding the current legal trends in privacy protection.

II. HABEAS DATA: THE MIDDLE GROUND FOR ENSURING PRIVACY OR A REFORMULATION OF AN ESTABLISHED PARADIGM?

Latin American countries have instituted legal mechanisms for the protection of data that substantively and procedurally differ from both those in the EU, the source of the privacy ideals, and from those in the United States, which continues to dominate the Western Hemisphere. Partially motivated by the privacy standards that the EU has established (complying with which is a prerequisite for a country's ability to exchange data with Union members), Argentina and several other Latin American countries have created a "new type of privacy protection" in the form of habeas data.[2]

While habeas data laws vary among Latin American countries, this right to information generally creates a private cause of action to insure compliance with constitutionally protected rights of "privacy . . . information self-determination and freedom of information."[3] Using this cause of action, individuals may seek relief in the form of destruction, correction, or an update of personal data.[4] The roots of

---

[1] *See* Press Release, Hanspeter Thur, Swiss Federal Data Protection Commissioner, 27th International Conference of Data Protection and Privacy Commissioners, Montreux (14-16 September 2005) (Sep. 16, 2005), *available at* http://www.edoeb.admin.ch/dokumentation/00438/00465/00888/00893/index.html?lang=en and 28th International Conference of Data Protection and Privacy Commissioners, *Welcome*, http://www.privacyconference2006.co.uk/index.asp?PageID=1 (last visited Sep. 16, 2006).

[2] Andrés Guadamuz, *Habeas Data: The Latin American Response to Data Protection*, 2001 J. INFO. L. & TECH. 3, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz (last visited Aug. 29, 2006).

[3] *Id.*

[4] *Id.*

habeas data are in Europe's privacy notions, and habeas data causes of action have been incorporated into the Constitutions of Argentina, Brazil, Paraguay, Peru, Ecuador, and Colombia during Latin America's post-Cold War democratization.[5]

The habeas data regime is at least partially a response to the polarized data protection regimes in the United States and the EU.[6] The EU has created top-down controls to assure the protection of personal data. The 1995 EU General Directive, which became effective in 1998, creates standards for the movement of personal data and calls upon member states to safeguard the "right to privacy with respect to the processing of personal data" and encourages the movement of information within the Union.[7] This Directive also prohibits the transfer of EU personal data to non-EU countries lacking adequate levels of personal data protection.[8] The Directive is meant to effectuate EU notions of privacy by regulating areas of personal data protection related to: "notice, choice, third-party use, security, data integrity, access, and enforcement."[9]

In contrast, the United States has taken an approach that utilizes a combination of "legislation, regulation, and self regulation."[10] In order to ensure that American companies were able to continue conducting business with European countries unhampered by the EU General Directive, the U.S. Department of Commerce worked with the EU to create a "Safe-Harbor" provision, which the EU approved in 2000.[11] By instituting privacy policies in compliance with the Safe Harbor, American companies maintain an adequate level of privacy

---

[5] *Id.*

[6] *See generally id.*

[7] Council Directive 95/46 On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 1, 1995 O.J. (L 281) 31, *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html [hereinafter EU Directive].

[8] *Id.*

[9] James D. Taylor & Terri J. Seligman, *European Union Privacy Directive*, NAT'L L. J., Aug. 14, 2000, at B10.

[10] U.S. Dep't of Commerce, Safe Harbor, http://www.export.gov/safeharbor/ (last visited Aug. 31, 2006).

[11] *Id.*

protection to continue conducting business requiring the collection of personal data with EU countries.[12]

Latin American countries, on the other hand, have generally selected the habeas data action approach to protect personal data, utilizing a system somewhere between self-regulation and adherence to strict, top-down standards.[13] However, the fact that countries like Argentina have promulgated privacy laws mirroring both the EU Directive and its complying national legislation, suggests that habeas data may not be enough to protect personal data—at least if one of the goals of protecting data is furthering economic viability and international competition. The push for greater regulation to comply with EU privacy standards in order to allow countries outside of the Union access to EU personal data in commercial settings is likely to increase privacy legislation in habeas data countries and make this cause of action just part of larger, national privacy regimes.[14]

III. ARGENTINA'S CONSTITUTIONAL FOUNDATION AND THE CATALYSIS OF CHANGE

The right to privacy is established in the Argentine Constitution, which creates several key concepts forming the basis of privacy law in Argentina.[15] Under the Constitution, the domicile, written correspondences, and private papers of individuals may only be searched and occupied in limited circumstances.[16] The "private actions" of individuals are considered outside the jurisdiction of the judiciary, provided they do not undermine public order, offend morality, or injure third parties.[17]

---

[12] *Id.*

[13] Guadamuz, *supra* note 2.

[14] *Id.*

[15] David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 15-16 (Fall 1999).

[16] CONST. ARG. art. 18. An English translation is available at http://pdba.georgetown.edu/Constitutions/Argentina/argen94_e.html.

[17] *See id.* art. 19.

In 1994, a new article dealing with privacy was added to the Constitution. It created the habeas data cause of action, allowing individuals to file suit to obtain information collected about them or to seek other forms of injunctive relief when false data about them has been collected or maintained, or discrimination occurred.[18] The habeas data provision manifested a "new generation of rights" and Argentina's effort to stay synchronized with "the international scenario and developments."[19] This provision creates the right to injunctive relief in the form of suppression of data, corrections or updates to the data, or an order to maintain the confidentiality of the data.[20] It empowers individuals to assess the information collected about them, scrutinize it for accuracy to assure that misleading information does not exist, and allows them to keep certain information undisclosed. Since habeas data actions may target information in either public or private databases,[21] both businesses and the government are thereby limited in their uses of private information and are subject to court-ordered alterations of these uses. By creating habeas data immunity for the media, which allows for maintenance of secret journalistic sources,[22] the Constitution declares that the benefits individuals may obtain by accessing their information are outweighed by the necessity of maintaining a free press. However, even this journalistic privilege, which creates habeas data immunity, is meant to be narrowly interpreted.[23] Therefore, while there are some exemptions for the media, these exemptions are afforded somewhat cautiously.

After the privacy article's incorporation into the Constitution, Argentina enacted privacy laws in reaction to invasions of privacy by

---

[18] *See id.* art. 43.

[19] Juan Antonio Travieso, Address at the International Working Group for Telecommunications 34th Annual Meeting in Berlin: Data Protection in Argentina: United or Unprotected 2 (Sept., 2003), *available at* http://www.datenschutz-berlin.de/infomat/heft31/Speech%20ProfTravesio.pdf (last visited Feb. 13, 2006).

[20] *See* CONST ARG., *supra* note 16, art. 43.

[21] *Id.*

[22] *Id.*

[23] *See Opinion of the Working Party on the Protection of Individuals with Regard to Processing of Personal Data: On the Level of Protection of Personal Data in Argentina*, at 6, (Oct. 3, 2002), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2002/wp63_en.pdf [hereinafter *Opinion of Working Party*].

the government. These laws, however, did not necessarily accomplish their purposes. For instance, when the government was attempting to ensure compliance with taxation laws in 1996, it scrutinized credit card, insurance, and tax records in the process.[24] To remedy this invasion of privacy, a reactionary bill passed allowing individuals to sue for invasion of privacy if their credit card histories had been reviewed.[25] Additionally, despite a Civil Code making it illegal to "arbitrarily interfere[ ] in another person's life: publishing photos, divulging correspondence, mortifying another's customs or sentiments or disturbing his privacy by whatever means,"[26] the invasion of privacy via wire-tapping has occurred—at least of high profile individuals.[27] Specifically, between 1990 and 1996, tapping the telephones of high government officials, including the President, was common. In addition, in 1998, the Mayor of Buenos Aires, who was a candidate in the 1999 Presidential election, lodged a complaint against a member of his own party and two city councilors for bugging his telephones and those belonging to his family.[28]

The push in Argentina to expand its protection of personal data beyond the habeas data action has come from a general international shift in data protection laws due to rapid technological innovation. As a result of

> increasing *electronic interpenetration* of previously distinct spheres of activity . . . greater attention will have to be given to protection of data not just on individual persons but *collective* entities. Greater attention will also have to be given to securing adequate quality not just of data and information but the *systems* used to process them.[29]

---

[24] Banisar & Davies, *supra* note 15, at 16.

[25] *Id.*

[26] COD. CIV., Art. 1071b is incorporated by Law No. 21.173, *cited in* Banisar & Davies, *supra* note 15, at 17.

[27] Banisar & Davies, *supra* note 15, at 16-17.

[28] *Id.*

[29] LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 13 (Kluwer Law International 2002).

In this landscape, legal attempts to expand Argentina's data protection began in 1996, but Parliamentary efforts were quashed by a strong financial lobby and a Presidential veto. This early initiative was largely based on the Spanish Data Protection Law of 1992 ("LORTAD")[30] and would have permitted individuals to access their personal data and prevented lending institutions from easily accessing credit histories in making lending decisions. Opposition to the initiative was also based on the fact that this new law would have restricted the exchange of information between various segments of the government and between Argentina and foreign countries.[31]

However, while this early legislative initiative failed, the international personal data protection standards changed due to the EU Directive and the increasing "global growth and promise of e-commerce [leading to the movement of] large quantities of personal information . . . across national borders in the context of transaction processing."[32] In 1998, Argentina successfully passed a law based on the European Directive,[33] severely restricting data transfers between the EU and other countries not adhering to EU standards.

IV. THE LAW FOR THE PROTECTION OF PERSONAL DATA

The Argentine Federal Senate passed the Law for the Protection of Personal Data ("LPPD") in 1998, and it went into effect with House approval in November 2000.[34] The Law is composed of 48 sections organized in seven statutory chapters. Only the final chapter deals

---

[30] Pablo A. Palazzi, *Data Protection in Latin American Countries*, http://www.ulpiano.com/DataProtectionEnglish.html. *See also* Antonio Mille & Maria del Rosario Mille, *Republic of Argentina*, *in* DATA PROTECTION LAWS OF THE WORLD VOLUME 1 OF 2, 1, 7 (Mark Ford & Clifford Chance eds. Feb. 2005).

[31] *Habeas Data: El Poder Ejecutivo Vetó Una Ley Cuestionada por los Bancos*, EL CLARIN DIGITAL, Dec. 31 1996, *available at* http://www.clarin.com/diario/96/12/31/o-01401d.htm.

[32] Joel R. Reidenberg, *E-Commerce and Transatlantic Privacy*, 38 HOUS. L. REV. 717, 718 (2001).

[33] *See* Law No. 25,326, Protection de los Datos, Oct. 30, 2000, *available in English* at http://www.privacyinternational.org/countries/argentina/argentine-dpa.html [hereinafter Law for the Protection of Personal Data].

[34] *See* Palazzi, *supra* note 30.

with habeas data actions.[35] The remaining chapters specify principles dealing with data protection and outline specific rights of data users and obligations of data owners.[36] The LPPD vests enforcement in a newly created controlling body[37] and establishes sanctions for violations.[38] The Law relies on executive regulations for its implementation[39] and applies retrospectively, that is, to all data banks existing at its inception.[40] While the LPPD as a federal law is enforceable throughout the country, provincial governments are invited to enact local regulations to assure compliance.[41] The only locality that has done so currently is the City of Buenos Aires.[42]

The enactment of the LPPD as a modification to the Constitutional right of habeas data has been "part of the global trend to protect citizens from the use that the public and private sectors can make of databases with personal information."[43] The Law was passed because the Constitution by itself was inadequate to enforce the right of privacy, and judges and attorneys needed further guidance regarding the enforcement of privacy rights in the context of personal data protection.[44]

---

[35] *See* Law for the Protection of Personal Data, *supra* note 33, ch. 7.

[36] *Id.* ch. 2-4.

[37] *Id.* ch. 5.

[38] *Id.* ch. 6.

[39] *Id.* § 45.

[40] *Id.* § 46.

[41] Decree No. 1558/2001, Dec. 2001, art 3, (Amy Bittner, trans.) *available in Spanish at* http://www.protecciondedatos.com.ar/dec1558.htm (on file with author) [hereinafter Decree].

[42] Mille & Mille, *supra* note 30, at 4.

[43] E-mail from Pablo Palazzi, Argentine attorney involved with the Foro de Habeas Data (www.habeasdata.org), to author (Jan. 26, 2006, 09:53 EST) (on file with author).

[44] *Id.*

A. HABEAS DATA ACTIONS UNDER THE LPPD

The LPPD provides the statutory framework for the habeas data right established in Article 43 of the 1994 Constitution and establishes the specifics of bringing a habeas data action.[45] It empowers individuals to seek injunctive relief by accessing their personal data kept in either public or private databases or by requesting that personal data be maintained confidential, suppressed, corrected, or updated.[46] Since the statute only codifies the constitutional right, the LPPD does not create a new cause of action. However, its elaboration of the constitutional right has altered some of the substantive rights. For instance, in accordance with the LPPD, a plaintiff is permitted to request that contested information be labeled as such during a legal proceeding, and the judge is permitted to grant provisional blocking of the information.[47] Similarly, the "any person" language in Article 43 of the Constitution,[48] referring to those with standing to bring habeas data claims, is clarified by the LPPD to include not only an affected person, but also a guardian, curator, or successor of that person.[49] Furthermore, while the Constitution establishes habeas data as a private cause of action absent involvement of a public interest, the LPPD seems to authorize broader government intervention on behalf of the plaintiff.[50]

The LPPD places considerable burdens on plaintiffs filing a habeas data complaint. Not only is the individual required to identify with as much precision as possible the name and domicile of either the data file or register and the data user, the plaintiff must also "attempt" to identify the appropriate government body if a public data bank is involved.[51] The plaintiff is also required to identify in his complaint

---

[45] *See* Law for the Protection of Personal Data, *supra* note 33, ch. 7.

[46] *Id.* § 33.

[47] *See id.*§ 38(3)-(4).

[48] *See* CONST ARG., *supra* note 16, art. 43.

[49] *See* Law for the Protection of Personal Data, *supra* note 33, § 34.

[50] *Id.*

[51] *Id.* § 38(1).

why he believes a particular database has information about him and reasons why that information is "discriminatory, false, or inaccurate" and must establish that the data owner is obliged to comply with the LPPD.[52]

While the standard for determining if the plaintiff has met these criteria is relatively low and therefore favorable to the plaintiff,[53] there may be instances when the plaintiff lacks the information necessary to demonstrate why he believes information in a data bank is "discriminatory, false, or inaccurate."[54] The level of specificity required is particularly problematic for plaintiffs initially seeking to access data they have never seen and therefore have no substantial reason to suspect that data's discriminatory, false, or inaccurate nature. At least part of this burden is alleviated by allowing the plaintiff to amend the complaint to include a request for "deletion, correction, confidentiality or updating" of personal data once the defendant has submitted a response to the original complaint.[55] The burden is then shifted to the defendant to demonstrate why the questioned information was included in the database and the reasons it refrained from providing the plaintiff's requested information.[56]

The LPPD also outlines a sanctions regime for infringements on the right of habeas data. The possible administrative sanctions include warnings, suspension, fines ranging between 1000 pesos and 100,000 pesos, or closing or canceling the data file, register or base.[57] The conditions and procedures for applying these sanctions are left open by the Law to subsequent regulations, but the penalties should be "graded in proportion to the seriousness and extent of the violation and the damages arising from such violations, guaranteeing the due process of law principle."[58]

---

[52] *Id.* § 38(2).

[53] *See id.* § 38(5).

[54] *See id.* § 38(2).

[55] *See* Law for the Proteciton of Personal Data, *supra* note 33, § 42.

[56] *Id.* § 41.

[57] *Id.* § 31(1).

[58] *Id.* § 31(2).

The LPPD also imposes criminal penalties under certain conditions, providing for incorporation of violations into the Argentine Criminal Code. For instance, knowingly inserting false information or having it inserted into a personal data file may lead to imprisonment of one month to two years.[59] When harm results from a habeas data violation, the punishment is increased by fifty percent.[60] Public officials are subject to a greater potential penalty. A special provision applying to convicted public officials automatically disqualifies them from office for a specified period of time.[61] The LPPD also imposes a penalty for breaking into a personal data bank or disclosing confidentially-registered data to a third party.[62]

The courts have been critical in clarifying the habeas data chapter of the LPPD. For instance, while the Law states that an action may be brought against both data bank users and those responsible for the data banks,[63] courts have expanded this to include "assignees" using the information.[64] Case law has also restricted the scope of habeas data actions, explaining that the object of the action is assessing the accuracy of the data.[65] This restriction starkly contrasts with the broad purpose of the Law: guaranteeing "honor and intimacy of persons, as well as the access to the information that may be recorded about such persons."[66] Trends visible in the most recent cases evidence the willingness of courts to compensate plaintiffs for emotional/subjective harm, find moral harm, increase the burdens on the defendant—even finding personal liability, and hear banking cases.[67]

---

[59] *Id.* § 32(1)(1).

[60] *Id.* § 32(1)(3).

[61] Law for the Proteciton of Personal Data, *supra* note 33, § 32(1)(4).

[62] *Id.* § 32(1)(2).

[63] *Id.* § 35.

[64] *See* Mille & Mille, *supra* note 30, at 19.

[65] *Id.*

[66] *See* Law for the Protection of Personal Data, *supra* note 33, § 1.

[67] Proteccion de Datos Personales, *Jurisprudencia*, (Amy Bittner trans.) *available in Spanish at* http://www.protecciondedatos.com.ar/, (on file with author).

B. GENERAL PROVISIONS AND PRINCIPLES OF THE LPPD AND THEIR RELATIONSHIP WITH THE EU DIRECTIVE

The EU has determined that in combination with the Argentine Constitution and Decree 1558/2001, the LPPD provides sufficient protections of privacy to conform to the European Union Directive.[68] In its explanation for accepting the Argentine Law as compliant, the EU focused on the existence of the habeas data cause of action established in Article 43 of the Constitution, the passage of the LPPD as a way to specify the right granted in the Constitution, and Regulation 1558/2001—providing enforcement mechanisms and interpretations of potential ambiguities.[69]

Dr. Juan Antonio Travieso, the head of the agency charged with administering the LPPD and overseeing data protection in Argentina, has suggested that Argentina's passage of the LPPD resulted from its perception of the global developments of privacy law:

> This is evidenced by the large number of States that have adopted legal norms related to data protection that are either similar or identical. It is therefore possible to state that we are witnessing an expansion of the contents and application of the international public order that includes personal data protection.[70]

Since Europe has been at the forefront of this movement, there are consequently many parallels between the LPPD and the EU Directive, but there are also some interesting differences. For example, both define "personal data," essentially, as information referring or relating to any physical or legal person.[71] However, while under the EU Directive personal data information includes information that can identify a person, especially if related to physical, mental, cultural, or

---

[68] *See generally Opinion of Working Party, supra* note 23.

[69] *Id.*

[70] Juan Antonio Travieso, *International Issues: Transfer of International Data. Applicable Law and Jurisdiction, available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/travieso_en.pdf (last visited Feb. 12, 2006).

[71] *Compare* Law for the Protection of Personal Data, *supra* note 33, § 2 *with* EU Directive, *supra* note 7, art. 2(a).

socio-economic identity, the Argentine Law creates a separate concept known as "sensitive data."[72] Under the LPPD, data is sensitive if it reveals racial or ethnic origin, religious, political, or philosophical beliefs, union membership, or information about health or sexual behavior.[73] Likewise, the "processing of personal data" definition in the EU Directive can be viewed as the predecessor to the definition of "data treatment" in the LPPD, with both focusing on any "operations" performed upon the data.[74] The LPPD also contains the concept of "data dissociation," a type of data treatment in which personal information is processed to make it difficult to match to its owner.[75]

The LPPD creates three categories of individuals: the "data owner," the "data user," and the "person responsible for the data file, register, bank or base."[76] The law is then written to govern the relationships between these groups.[77] The Directive's "data subject"[78] is described similarly to the LPPD's "data owner" ("[a]ny physical person or legal entity . . . whose data are subject to the treatment referred to in this Act.").[79] The "controller"[80] under the EU Directive is similar to the "person responsible"[81] under the LPPD. While the EU Directive divides those with access to data and working with it into categories of "processor" and "third party,"[82] the LPPD simply defines a "data user" as someone "performing . . . the treatment of data . . .

---

[72] *Id.*

[73] *See* Law for the Protection of Personal Data, *supra* note 33, § 2.

[74] *Compare* Law for the Protection of Personal Data, *supra* note 33, § 2 *with* EU Directive, *supra* note 7, art. 2(b).

[75] *See* Law for the Protection of Personal Data, *supra* note 33, § 2.

[76] *See Id.*

[77] *Id.*

[78] *See* EU Directive, *supra* note 7, art. 2(a).

[79] *See* Law for the Protection of Personal Data, *supra* note 33, § 2.

[80] *See* EU Directive, *supra* note 7, art. 2(d).

[81] *See* Law for the Protection of Personal Data, *supra* note 33, § 2.

[82] *See* EU Directive, *supra* note 7, arts. 2(e)-(f).

owned by such persons or to which they may have access through a connection."[83]

The purpose of the LPPD is more precise than the purpose articulated in the Directive. The Directive just requires and enables member states to "protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data."[84] The purposes of the Argentine Law, on the other hand, is to fully protect personal information contained in public or private data treatment mechanisms used in providing reports, protect the honor and intimacy of individuals, and provide persons with access to their information in accordance with Article 43 of the Constitution.[85] Protections afforded to individuals by the LPPD are also available to legal entities.[86] Thus, while the EU countries are not required to afford similar personal data protections to corporations, even though some countries like Austria, Denmark, and Italy do so anyway,[87] the Argentine Law requires it. Additionally, neither the data protection provisions of the Directive nor the LPPD apply to journalistic sources.[88]

C. RIGHTS AND OBLIGATIONS

The principles forming the backbone of the LPPD are similar to the principles of the EU Directive. Just like those of the EU Directive,[89] the principles of the LPPD focus on the quality of the data, empowering the data owner to obtain information and provide consent, and placing obligations upon the data user and the person responsible

---

[83] *See* Law for the Protection of Personal Data, *supra* note 33, § 2.

[84] *See* EU Directive, *supra* note 7, art. 1.

[85] *See* Law for the Protection of Personal Data, *supra* note 33, § 1.

[86] *Id.*

[87] *See* MARK FORD, EDWARD N. JACKSON, & CLIFFORD CHANCE, *in* DATA PROTECTION LAWS OF THE WORLD VOLUME 1 OF 2, 1, 7 (Mark Ford and Clifford Chance eds. Mar. 2004).

[88] *Compare* Law for the Protection of Personal Data, *supra* note 33, § 1 *with* EU Directive, *supra* note 7, art. 9.

[89] *See* EU Directive, *supra* note 7, art. 6(1).

for the data.[90] The principles relating to data quality in the Directive are echoed in Sections 3 and 4 of the LPPD, which focus on the lawfulness and quality of the data. The LPPD, adhering to the EU Directive, requires lawful formation of data files.[91] It requires that data collected about persons be "certain, appropriate, pertinent, and not excessive,"[92] as well as accurate and updated,[93] limited in purpose,[94] and destroyed when no longer necessary.[95] However, the LPPD creates requirements for the quality of data not reflected in the Directive. For instance, the Argentine Law mandates that the data owner must have a right to access the data.[96]

To actualize these principles, under the LPPD the data owner is empowered primarily through the consent provision, which provides that the treatment of data is unlawful when done without the express, written consent of the data owner.[97] Despite this consent provision, treatment of data without consent is permitted in several situations, such as when the information collected is (1) public, (2) meant to perform the inherent duties of the state, (3) limited, or (4) arising out of a contractual relationship.[98] The LPPD also empowers data owners by requiring express notification whenever anyone requests his or her personal data.[99] Before such information may be disclosed to the requesting party, the data owner must be notified of the purpose for the requested data treatment; how compulsory providing the information requested is; and the consequences of providing, refusing,

---

[90] *See* Law for the Protection of Personal Data, *supra* note 33, ch. 2.

[91] *Id.* § 3.

[92] *Id.* § 4(1).

[93] *Id.* § 4(4).

[94] *Id.* § 4(3).

[95] *Id.* § 4(7).

[96] Law for the Proteciton of Personal Data, *supra* note 33, § 4(6).

[97] *Id.* § 5.

[98] *Id. See also, Opinion of Working Party, supra* note 23, at 16 (for criticism by EU).

[99] *See* Law for the Protection of Personal Data, *supra* note 33, § 6.

or inaccurately providing the information.[100] The LPPD also protects individual data owners because it forbids compelling the collection of sensitive data. Only lawful, competent authorities can manipulate such sensitive data if there exists both a "general interest authorized by law" and the data owner is not identifiable.[101]

The rights vested in the data owner are the right to information,[102] the right to access,[103] and the right to rectification, updating, or suppression.[104] The right of information simply allows data owners to inquire about and confirm the existence of their personal data, and creates a right to know the purpose for which that data is kept, as well as disclosure of the parties responsible for it.[105] The right of access, on the other hand, actually permits data owners to request and obtain their personal information and requires data users or persons responsible to provide it within ten days or face a potential habeas data action.[106] The right of access also allows data owners to inquire about the purpose for which and the methods in which the personal data was obtained and its destination.[107] The information provided to the data owner must be comprehensive and must be communicated clearly in the format most convenient for the data owner.[108] The "rectification, updating, or suppression" right, in contrast, creates a right for data owners to control the accuracy and amount of information available about them and places an obligation upon the data user or party responsible to either correct or keep confidential information upon the

---

[100] *Id.*

[101] *Id.* § 7.

[102] *Id.* § 13.

[103] *Id.* § 14.

[104] *Id.* § 16.

[105] Law for the Proteciton of Personal Data, *supra* note 33, § 13.

[106] *Id.* § 14(2).

[107] Decree, *supra* note 41, art. 14.

[108] *See* Law for the Protection of Personal Data, *supra* note 33, § 15.

data user's request.[109] The consequence of non-compliance is a potential habeas data claim.[110]

The LPPD provides very narrow exceptions for when these rights may be refused to the data owner, thereby providing the data user or the person responsible for the data a legitimate defense in the event of a habeas data action. The data user or person responsible for the data may deny a data owner's request to obtain, correct, or maintain the confidentiality of data only upon a "well grounded decision" based on "national defense, public order, and safety . . . or the protection of rights and interests of third parties."[111] If a public data register or bank holds the information, access may also be properly denied when it could adversely affect pending proceedings related to tax or social security obligations, health and environmental functions, or the investigation of crimes.[112]

The Law also places numerous obligations upon the data user. For instance, there is a non-delegable duty upon anyone treating data to maintain its confidentiality,[113] and data users are required to take "measures as are necessary to guarantee the security and confidentially of personal data."[114] Communication of personal data by data users is conditioned upon the revocable consent of the data owners and must advance a legitimate purpose.[115]

The LPPD's regulation of international transfers was modeled on Article 25 of the EU Directive, and provides no safe harbor provision for the U.S. for transferring information to and from Argentina.[116] It prohibits the transfers of personal data to countries with inadequate

---

[109] *See id.*§ 16.

[110] *Id.*

[111] *Id.* § 17(1).

[112] *Id.* § 17(2).

[113] *Id.* § 10(1).

[114] Law for the Proteciton of Personal Data, *supra* note 33, § 9(1).

[115] *Id.* § 11.

[116] Morrision & Foerster, *Privacy and Transborder Transfer of Personal Data—Latin America*, (Nov. 2000), http://www.mofo.com/news/updates/files/update169.html.

levels of protection.[117] However, this general rule does not apply, and data may therefore be transferred internationally, regardless of adequacy of protection in the other country (a) in areas of international judicial cooperation; (b) when dealing with medical information needed to treat the data owner or for survey purposes, provided anonymity is maintained; (c) during stock exchanges and bank transfers; (d) in accordance with Argentine treaties; or (e) for international cooperation between agencies fighting "organized crime, terrorism, and drug-trafficking."[118] Data owners, however, may choose to expressly consent to the transfer of information to a country not considered adequate.[119]

Argentina has not yet enacted a list of countries considered adequate, nor is there a list of countries presumed inadequate.[120] Attorneys are consulted on these issues and La Direccion Nacional de Proteccion de Datos Personales ("DNPDP"), the agency charged with enforcing data protection, assists companies in establishing contracts for the transfer of personal data. Currently "they are being very cautious in labeling a country as adequate or not adequate."[121] As of yet there are no cases examining these issues. Due to their complexity little attention is paid to them in the press, since the LPPD "is modeled upon the Spanish LORTAD and the EU Directive . . . European legislation is going to be considered adequate in light of this historical origin."[122] Regulation 1558/2001 gives some guidance in this area. In determining adequacy, all of the circumstances involved in an international transfer or series of transfers must be considered.[123] Determining the appropriateness of an international transfer includes weighing the nature of the information, its finality and duration, the place of final destination, the laws of the country processing the

---

[117] *See* Law for the Protection of Personal Data, *supra* note 33, § 12(1).

[118] *Id.* § 12(2).

[119] Decree, *supra* note 41, art. 12.

[120] E-mail from Pablo Palazzi, *supra* note 43.

[121] *Id.*

[122] *Id.*

[123] Decree, *supra* note 41, art. 12.

information as well as the country's norms, codes of professional conduct, and security.[124]

D. THE CONTROLLING BODY AND ENFORCEMENT

The LPPD created a controlling body, the DNPDP, to oversee the personal data legal regime, charging it with taking the actions necessary to actualize the provisions of the LPPD and outlining several of its functions.[125] The DNPDP is an agency of the Ministry of Justice and Human Rights, is currently under the direction of Dr. Juan Antonio Travieso.[126] Its funding comes primarily from taxes collected for services that it provides and also from the national budget.[127] Travieso stated that the goal of the DNPDP is to "achieve the advantages of Internet in Argentina, by means of liasing organisations [sic] and individuals that can also announce a new era of social communication."[128]

The DNPDP's functions include pending requesting parties advice and assistance in understanding the LPPD, promulgating applicable rules and regulations, maintaining records of data files, enforcing administrative sanctions, monitoring private depositories, and standing in the place of the accuser in habeas data actions.[129] The Agency is charged with maintaining the records of habeas data judgments as well.[130] The DNPDP must also, upon the request of an interested party, investigate the legality of the gathering, exchanging, delivering, and controlling of personal data.[131] The EU has questioned the independence of the DNPDP Director because he is both nominated

---

[124] *Id.*

[125] *See* Law for the Protection of Personal Data, *supra* note 33, § 29.

[126] Ministrio de Justicia y Derechos Humanos, *La Direccion Nacional de Protección de Datos Personales*, http://www2.jus.gov.ar/dnpdpnew/ (last visited Aug. 3, 2006).

[127] Decree, *supra* note 41, art. 29(3).

[128] Travieso, *supra* note 19, at 5.

[129] *Id.*

[130] *See* Law for the Protection of Personal Data, *supra* note 33, § 43(4).

[131] Decree, *supra* note 41, art. 4.

and may be dismissed by the Minister of Justice and Human Rights.[132] The EU has also expressed concern about the effectiveness of DNPDP because it only has federal jurisdiction and no power when a matter falls within the jurisdiction of an Argentine province.[133]

Through regulations, the DNPDP attempts to strike a balance between the private and public interests involved in privacy regulation. For instance, its Advisory Board, vested with the responsibility of advising the Director on privacy issues, includes representatives from the Ministries of Justice and Human Rights and of the Fiscal Public Ministry, a Bicameral representative, representatives from the business community, the central bank, and the credit card industry.[134] However, while various interests are involved in the advisory process, the Director retains broad authority and full independence.[135]

Registering with the DNPDP is required of any data depositories[136] and private data banks.[137] Registration requires the inclusion of specific information, like the name and domicile of the person in charge of the data, the purpose and characteristics of the data file, the nature of the data and the form in which it must be collected and updated, entities who may receive it, ways in which the data is to be secured, categories of people with access to it, the length of time for which it will be utilized, and the conditions under which data owners will have rights to access and update the data.[138] The data possessed by the user must conform to its description in the register.[139]

The DNPDP may be the key in providing the framework for similar institutions and similar data protection laws in other parts of Latin America. Travieso has emphasized the critical role that his country and the Agency may play in Latin America in the near future.

---

[132] *See Opinion of Working Party, supra* note 23, at 14.

[133] *Id.*

[134] Decree, *supra* note 41, art. 29(4).

[135] *Id.* art. 29(1).

[136] *See* Law for the Protection of Personal Data, *supra* note 33, § 21.

[137] *Id.* § 24.

[138] *See id.*§ 21(2).

[139] *Id.* § 21(3).

He hopes to further develop the Latin American Data Protection Network, similar to the Argentinean Data Protection Network, begun in 2003 to assure compatibility of data protection laws.[140] Argentina may play a key role, especially because of its experience with the EU and its pioneering in Latin America to harmonize personal data protection policies, "essential for [the] region and its always interesting and vast market."[141]

V. CONCLUSION

Until relatively recently, the protection of personal data has been handled globally using one of two main approaches: regulation, as in the EU, or free-market forces, as in the United States. The need to protect personal data has been accepted and transformed in Latin America. The origins of protections were the creation of the habeas data rights in the Constitutions of several Latin American countries, including Argentina. However, the need to simultaneously protect personal data in the face of advancing technology, and to maintain economic compatibility on an international scale, have contributed to Argentina's decision to pass the LPPD and thereby provide data protection in accordance with the EU model. Due to the passage of the LPPD, "[c]ompanies and public officials are more concerned about the uses of the personal information in their hands. They are aware that people can exercise their rights at any time[, so] they pay attention to the law."[142] Since banks and companies are being sued for non-compliance, which constantly makes the news, the debate has also surfaced in the press.[143] As countries follow Argentina's example, the EU model may quickly set the standards and expectations for data protection worldwide.

---

[140] Travieso, *supra* note 19, at 13.

[141] *Id.* at 14.

[142] E-mail from Pablo Palazzi, *supra* note 43.

[143] *Id.*